WHAT IS CLAIMED IS:

1. A method for obtaining a printed copy of a document at a printer from a server via a client, the method comprising the steps of:

installing a private encryption key in the printer, the private encryption key being unavailable to the client and the server;

providing the server with a public encryption key, the public encryption key being associated with the private encryption key, the public encryption key being different than the private encryption key;

receiving an encrypted file at the printer from the server via the client, the encrypted file being encrypted using the public encryption key;

generating decrypted data associated with the document by decrypting the encrypted file in the printer using the private encryption key; and

printing the document at the printer using the decrypted data.

2. A method as defined in claim 1, wherein the step of installing a private encryption key in the printer comprises the step of installing the private encryption key in a tamper resistant electrical module.

3. A method as defined in claim 1, wherein the step of installing a private encryption key in the printer comprises the step of installing the private encryption key in a replaceable ink cartridge.

4. A method as defined in claim 1, wherein the step of providing the server with a public encryption key comprises the step of retrieving the public encryption key from the printer.

5. A method as defined in claim 1, wherein the step of providing the server with a public encryption key comprises the step of transmitting the public encryption key from the client to the server.

6. A method as defined in claim 1, wherein the step of providing the server with a public encryption key comprises the step retrieving the public encryption key based on a unique identification code associated with the printer.

7. A method as defined in claim 1, wherein the step of providing the server with a public encryption key comprises the step retrieving the public encryption key based on a unique identification code associated with a print cartridge.

8. A method as defined in claim 1, wherein the step of providing the server with a public encryption key comprises the step retrieving the public encryption key from a certification authority based on a serial number retrieved from the printer.

9. A method as defined in claim 1, wherein the step of providing the server with a public encryption key comprises the step retrieving the public encryption key from a certification authority based on a serial number retrieved from a print cartridge.

10. A method as defined in claim 1, further comprising the step of transmitting a request for the encrypted file from the client to the server.

11. A method as defined in claim 1, wherein the step of generating decrypted data associated with the document by decrypting the encrypted file in the printer using the private encryption key comprises the step of using the private encryption key indirectly by:

using the private encryption key to decrypt an encrypted session key; and

decrypting the encrypted file using the decrypted session key.

12. A method as defined in claim 1, wherein the step of generating decrypted data associated with the document by decrypting the encrypted file in the printer using the private encryption key comprises the step of decrypting the entire encrypted file using the decrypted symmetric encryption key directly.

13. A printer for printing a copyrighted document based on encrypted data received via the Internet, the printer comprising:

a communication port operatively coupled to the Internet;

a memory device storing an embedded encryption key, the embedded encryption key being unavailable outside the printer;

a decryption module electrically coupled to the communication port and the memory device, the decryption module being adapted to receive an encrypted version of the copyrighted document via the communication port, the decryption module being adapted to convert the encrypted version of the copyrighted document into decrypted data indicative of the copyrighted document using the embedded encryption key; and

a printing mechanism operatively coupled to the decryption module, the printing mechanism being adapted to receive the decrypted data and print the copyrighted document based on the decrypted data.

14. A printer as defined in claim 13, wherein the communication port is electrically coupled to a client device.

15. A printer as defined in claim 13, wherein the communication port is electrically coupled to a document server via the Internet.

16. A printer as defined in claim 13, wherein the embedded encryption key comprises an asymmetric private encryption key.

17. A printer as defined in claim 13, wherein the embedded encryption key comprises an symmetric session key.

18. A printer as defined in claim 13, further comprising a controller operatively coupled to the communication port and the printing mechanism, the controller being adapted to receive non-encrypted data indicative of a non-copyrighted document from the communication port, the controller being adapted to transmit control signals to the printing mechanism to print the non-copyrighted document.

19. A printer as defined in claim 13, wherein the decryption module comprises a tamper resistant housing.

20. A printer as defined in claim 13, wherein the decryption module comprises a replaceable ink cartridge.

21. A printer as defined in claim 20, wherein the replaceable ink cartridge comprises a tamper resistant housing.

22. A printer as defined in claim 20, wherein the private key is inaccessible outside the replaceable ink cartridge.

23. A printer as defined in claim 13, wherein the decryption module comprises a smartcard.

24. A printer as defined in claim 13, wherein the memory device stores a public encryption key, the public encryption key being electronically accessible via the communication port.

25. A printer as defined in claim 13, wherein the memory device stores a serial number, the serial number being electronically accessible via the communication port.

26. A printer as defined in claim 13, wherein the decryption module is adapted to receive an encrypted session key from the communication port, the decryption module being adapted to decrypt the encrypted session key using the embedded encryption key, the decryption module being adapted to employ the decrypted session key during conversion of the encrypted version of the copyrighted document into decrypted data.

27. A printer as defined in claim 13, wherein the printing mechanism comprises a plate maker.

28. A printer as defined in claim 13, wherein the printing mechanism comprises a film recorder.